스마트폰에서 mVoIP 취약성 분석 및 대응 방안

조식완, 장원준, 이형우*
한신대학교 컴퓨터공학부

mVoIP Vulnerability Analysis And its Countermeasures on Smart Phone

Sik-Wan Cho, Won-Jun Jang, Hyung-Woo Lee*
School of Computer Engineering, HanShin University

요 약 mVoIP 서비스는 IP 네트워크를 이용하여 모바일 장비에서 음성 정보를 보다 효율적으로 전송할 수 있는 기술이다. mVoIP 서비스는 적은 통신 비용으로도 다양한 부가서비스를 제공할 수 있으며, IP 기반 네트워크를 이용하여 효율성과 가용성을 높일 수 있는 방식이다. 또한 일반 사용자는 시간과 장소에 상관없이 모바일 장비에서 음성 대화 서비스를 이용할 수 있다는 장점이 있다. 하지만, 모바일 장비에서의 SIP 프로토콜은 도청, DoS 공격 및 오작동, 스맵 공격 등과 같은 다양한 공격과 위협에 노출되어 있어 많은 문제점으로 대두되고 있다. 이에 본 연구에서는 기존 mVoIP 서비스에 대한 위협과 취약성에 대해 분석하여 다양한 형태의 공격 시나리오를 도출하였다. 공격 시나리오에 대한 보안 취약성을 분석하여 보다 안전한 SIP 메커니즘을 제시하였으며 모바일 환경에서의 취약성을 제거할 수 있는 대응 방안을 제시하였다.

• **주제어** : 스마트폰, 모바일브이오아이피, 취약성, 응답 메커니즘, 보안

Abstract mVoIP (mobile Voice over Internet Protocol) service is a technology to transmit voice data through an IP network using mobile device. mVoIP provides various supplementary services with low communication cost. It can maximize the availability and efficiency by using IP-based network resources. In addition, the users can use voice call service at any time and in any place, as long as they can access the Internet on mobile device easily. However, SIP on mobile device is exposed to IP-based attacks and threats. Observed cyber threats to SIP services include wiretapping, denial of service, and service misuse, VoIP spam which are also applicable to existing IP-based networks. These attacks are also applicable to SIP and continuously cause problems. In this study, we analysis the threat and vulnerability on mVoIP service and propose several possible attack scenarios on existing mobile VoIP devices. Based on a proposed analysis and vulnerability test mechanism, we can construct more enhanced SIP security mechanism and stable mobile VoIP service framework after eliminating its vulnerability on mobile telephony system.

• **Key Words** : Smart Phone, mVoIP, Vulnerability, Response Mechanism, Security

1. 서론

인터넷 전화 서비스는 기존 인터넷망을 이용하여 음성/영상을 전송하는 방식으로 일반 전화망과 인터넷 망의 연동이 가능한 멀티미디어 통신서비스 기술이다. 기존에는 H.323 방식이 주로 이용되었지만, 현재는 보다 간

본 논문의 일부 내용은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2012R1A1A2004573)
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2012년 6월 5일 수정일 2012년 7월 18일 게재확정일 2012년 8월 25일

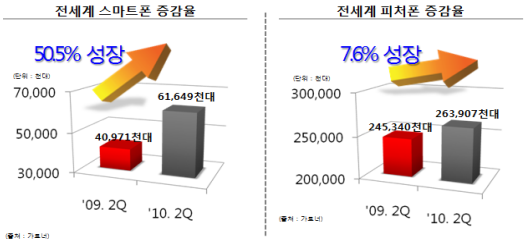
편하고 확장성과 효율성을 제공하는 SIP(Session Initiation Protocol) 프로토콜 기반의 인터넷 전화 서비스가 주로 이용되고 있다. 최근 Apple 社의 iPhone 등과 같은 스마트폰이 선풍적인 인기를 끌면서, WiFi를 이용하여 무선 AP가 설치되어 있는 곳이면 모바일을 이용한 무선 인터넷을 무료로 즐길 수 있게 되었으며, 모바일 환경에서의 인터넷 전화 서비스 이용 역시 급증 하였다. 스마트폰은 어플리케이션의 설치와 삭제가 사용자에 의해 조정될 수 있고 ROM/RAM이 존재하는 모바일 PC의 기능이 있는 폰을 의미한다. 기본적으로 무선랜이 장착되어 있어 인터넷에 접속이 가능한 것은 물론 멀티 테스킹의 기능이 일반 휴대폰에 비해 용이하며 레지스트리 편집이나 문서 작성/ 엑셀 등 PC에서 구동되는 기본 프로그램을 활용할 수 있는 손안의 작은 PC 같은 멀티기기 역할을 하는 폰을 스마트폰이라고 한다. 하지만 이러한 편의성 때문에 VoIP 스팸 공격 및 불특정 다수의 Call Dos 공격, 개인정보 유출, 악성코드 유포 등 mVoIP 서비스에 대한 취약성을 이용한 공격들이 생겨나고 있으며 그 정도가 점차 지능적이고 고도화 되어가고 있다. 특히 mVoIP 기반 모바일 단말에서 사용하는 SIP 프로토콜은 보안성이 취약한 프로토콜이므로 프로토콜 송수신 패킷에 대해 쉽게 위변조가 가능하고 송신자 인증기능에 문제점이 발견되고 있으며, 모바일 단말을 이용한 국제 인터넷 전화 스팸 발생 등도 가능하며, 국내 모바일 VoIP 서비스 이용 시 악의적인 공격자에 의해 콜포킹, 컨퍼런스 콜 도감청 및 컬러링 서비스 오용공격 등과 같은 SIP 기반 부가서비스 공격 등이 가능하기 때문에 대응 기술에 대한 연구가 시급하다. 이러한 공격기법의 근본적인 문제는 공격자가 정상적인 통신 패킷을 수정 및 삭제하고 이를 변경하는데 문제가 없기 때문에 발생한다. 현재까지 수행된 대부분의 연구는 각기 PC에서의 VoIP 환경 또는 일반 모바일 환경을 대상으로 한 취약성 분석이었기 때문에 스마트폰과 같이 모바일과 VoIP가 통합된 네트워크 환경에 대한 연구가 필요하다.

따라서 본 연구에서는 스마트폰의 mVoIP환경에서 Call Flow 및 mVoIP 서비스의 취약성에 대해 분석하고, 보다 실질적인 취약성 분석을 위해 스마트폰 환경에서 제공되고 있는 VoIP 부가서비스를 이용하여 구체적인 대응 방안을 제시하였다.

2. mVoIP 서비스

2.1 mVoIP

mVoIP(Mobile Voice over Internet Protocol)는 이동전화 단말과 3G, WiBro, Wi-Fi 등 무선 네트워크에 기반한 인터넷 전화 서비스를 말한다.



[Fig. 1] Market Trends

mVoIP 서비스는 현재 스마트폰을 중심으로 급격히 증가하고 있다. VoIP 자체가 저렴한 통신비용을 자칭하고 있음은 물론이거니와 스마트폰 자체에서 제공하는 편의성으로 인해 사용량이 급격하게 증가하고 있다.

2.2 mVoIP 표준 SIP 프토로콜

mVoIP에서 사용되는 기술 중, 현재 표준으로 널리 사용되는 SIP는 어떠한 프로토콜 스택에 의존적이지 않고, HTTP(HyperText Transfer Protocol)와 같은 텍스트 기반으로 정의되어 있어 확장이 용이하며, 경량화 되어 있고, 쉽게 사용할 수 있는 프로토콜이다. SIP는 대체적으로 호를 연결하기 위한 시그널링 프로토콜로 많이 쓰이며, 위치 지정 메시지를 통해 이동성을 제공하므로, mVoIP 서비스에 적합한 기술이라 할 수 있다.

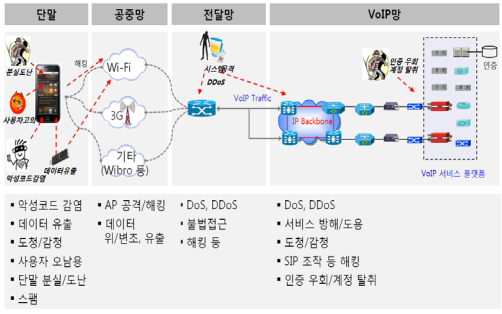
SIP는 클라이언트들이 호출을 시작하면 서버가 그 호출에 응답을 하는 클라이언트/서버 구조에 기반을 두고 있다. SIP는 이러한 기존의 텍스트 기반 인터넷 표준들에 따름으로써, 고장 수리와 네트워크 디버깅 등이 쉽다. SIP 통신의 세션 설정 및 통신 과정은 사용자가 Proxy 서버에 등록하는 과정부터 시작하여 호 연결 및 해제 요청을 한다.

2.3 스마트폰에서의 mVoIP 취약성

스마트폰에서 제공하고 있는 mVoIP 서비스는 주요 특성 중 하나인 편의성과 저렴함 때문에 대표적인 통화 서비스로 급부상하여 자리매김할 가능성이 크다.

mVoIP에서 주로 다루는 SIP는 설계 당시 보안적인 요소가 고려되지 않아 항상 위협에 노출되어 있다. 실제로 SIP를 대상으로 하는 다양한 공격들이 가능하다. 대표적인 SIP 공격기법으로는 다음과 같다.

[Fig. 2] Security Threats on Smartphone



[Fig. 3] mVoIP Attack Mechanism

3. mVoIP 취약성 분석

3.1 INVITE Packet

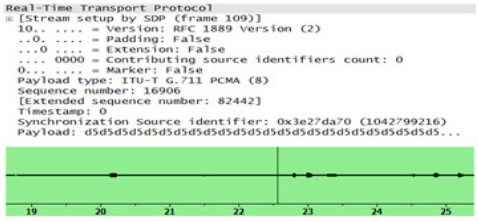
INVITE 패킷은 통화 연결 시 초기에 쓰이는 패킷으로 통화 연결과정에서 제울 중요한 패킷이 INVITE 패킷이다. INVITE 안의 메시지를 통해 송수신자의 정보 및 연결요청 상태를 알 수 있으며 특히 부가서비스 등록 및 해제의 경우 송신자가 어떠한 부가서비스를 요청하였는지에 대해서도 INVITE 패킷을 통해 알 수 있다.

또한 몇몇 부가서비스의 경우 INVITE 패킷 안에 XML 메시지가 담겨있는 경우도 있기 때문에 공격자가 INVITE 패킷을 감지 및 내용을 변조하는 공격을 하였을 경우 피해 정도가 커질 수 있다. 결국 공격자에 의해서 INVITE 패킷이 일반 사용자 대신 보내질 경우 연결 대상에 대한 공격이 가능하게 된다.

[Fig. 4] Weakness of INVITE Packet

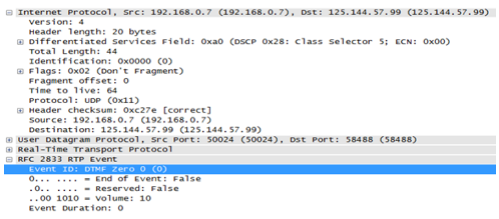
3.2 RTP Packet

RTP 패킷은 VoIP에서 음성과 영상데이터를 전달해주는 역할을 하는 프로토콜이다. 즉, RTP 패킷을 통해 도감청 및 음성과 화상 데이터를 위변조 할 수 있게 되는 것이다.



[Fig. 5] RTP based Wiretapping Attack

또한 국내에서 제공하는 일부 안내 서비스에서 안내에 맞춰 스마트폰 단말기의 버튼을 눌렀을 경우, 눌렀을 때의 번호 데이터가 RTP 형태로 지나가게 하는 형태의 서비스도 있다. 이 같은 경우 단말기의 눌렀던 번호가 암호화되어 있지 않아 그대로 노출되어 있기 때문에 피해가 커질 수 있다.



[Fig. 6] RTP Packet after Press 0 on Keypad

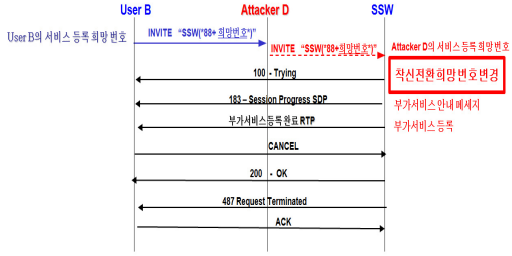
3.3 패킷 내 XML 메시지 내용 변경

몇몇 부가서비스에 쓰이는 패킷 안에는 XML 메시지가 들어있다. 이 XML 메시지 안에는 수신자에 대한 정보나 현재 상태 등이 들어가 있으며 수집 및 내용 변경이 용이하기 때문에 공격자에 의해 내용이 변조되었을 시

원치 않는 수신자와 통화하거나 통화 연결 방해 등의 피해를 받을 수 있다.

[Fig. 7] XML Message on INVITE Packet

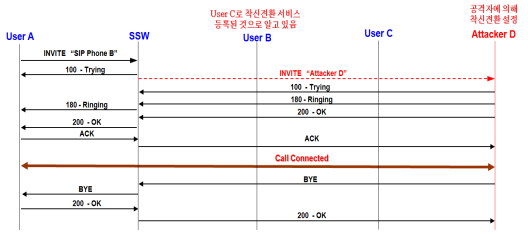
이 밖에도 다양한 형태의 공격이 가능하다. 부가서비스 중에 하나인 착신 전환 서비스인 경우 착신 전환 서비스 패킷에 대한 송신자 인증 과정이 없으며 희망 번호에 대한 확인이나 검증 과정이 없는 문제점을 이용하여 공격자가 공격대상에 대한 정보를 가지고 있을 시 이를 이용해 공격대상을 사칭하여 SSW에 착신전환 서비스 등록이 가능하다. 또한 공격자가 임의의 사용자들에 대한 정보를 가지고 있을 시 착신전환 서비스를 이용하여 수신된 전화를 특정 공격대상 번호로 착신 전환이 가능하다.



[Fig. 8] Roaming Service Modification Attack

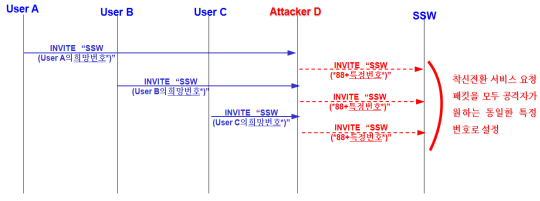
이 같은 공격을 하기 위해서는 먼저 공격대상에 대한 정보가 있어야 하므로 공격대상의 패킷을 캡처한 후 캡처된 내용을 바탕으로 각 공격 대상들의 정보를 테이블이나 DB에 저장한다. 공격대상이 착신전환 서비스를 신청할 때 공격대상의 희망번호가 등록되어 있는 정상적인 착신전환 서비스 요청 패킷을 공격자 희망번호가 적인 변조된 착신전환 서비스 요청 패킷으로 변조한다. 그 후 변조된 INVITE 패킷을 SSW에 전송하여 공격대상의 착신전환 서비스가 공격자 희망번호로 등록되게 한다. 이로 인하여 공격대상의 번호로 통화연결 시 SSW는 공격자 희망번호로 연결해준다.

또한 다음과 같이 착신전화 서비스 공격자 위장 등록도 가능하다. 착신전환 부가서비스 요청 시 서비스 등록하는 공격대상의 희망번호를 공격자 희망번호로 변경하는 것이 아니라 공격자 자신으로 등록하여 공격대상으로 전화 연결 시 공격자로 연결되게 하는 공격을 의미한다.



[Fig. 9] Masquerading Connetion Attack

이밖에도 착신전환 서비스를 이용하여 DDoS 공격도 수행할 수 있다. 공격 대상들의 착신전환 서비스 희망 번호가 담긴 INVITE 패킷을 공격자가 원하는 공격대상 번호가 담긴 INVITE 패킷으로 변조하여 SSW에 전송한다. 한편 공격자에게 INVITE 패킷을 받은 SSW는 착신전환 서비스 데이터베이스에 각 공격 대상들의 착신 희망번호가 아닌 공격자의 공격대상 번호로 등록하게 된다. 이후 각각 공격 대상들에게 연결하고자 하는 발신자들은 모두 공격자가 등록해놓은 또다른 공격대상 번호로 연결하게 되며 공격자에 의해 SSW에 등록된 공격대상은 착신전환 설정이 집중되어 있기 때문에 통화량이 폭주하는 DDoS 형태의 공격이 가능하다는 문제점이 발생한다.



[Fig. 10] DDoS Attack on Roaming Service

이와 같이 현재 모바일 단말에서 사용 가능한 mVoIP 기반 인터넷 전화 서비스에는 다양한 형태의 보안 취약성이 발견되고 있어서 이에 대한 대응 기법 등에 대한 연구가 필요하다. 이에 본 연구에서는 우선 다음과 같은 방법을 제시하고자 한다.

4. mVoIP 취약성 대응 방안

4.1 OTD(One Time Digit)

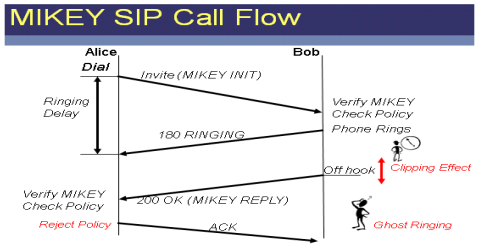
OTD는 OTP(One Time Password)와 유사한 개념으로 말 그대로 일회용 디지털 키를 이용하여 인증기법을 강화하는 방식이다. 먼저 송신자에서 INVITE 패킷을 보

내게 되면 서버에서는 이를 이용하여 랜덤 비트열의 일회용 키를 만들어 전송한다. 이에 송신자는 일회용 키가 적용된 INVITE 패킷을 다시 전송하게 되고 서버는 킷값 인증을 통해 이후 연결과정을 진행하는 형태이다.

이 같은 형태의 인증 방식은 Replay Attack을 사전에 차단할 수 있으며 정상적인 형태로 위조된 SIP 패킷에 대해서도 차단하고 이후 연결과정을 진행하기 때문에 기밀성과 무결성을 제공하는 장점이 있다.

4.2 MIKEY(Multimedia Internet KEYing)

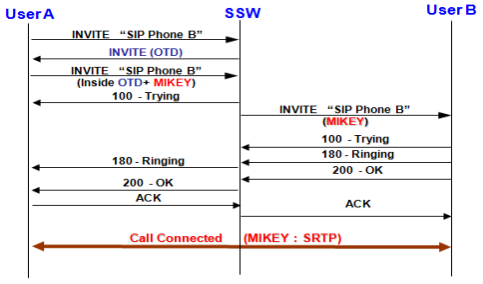
MIKEY는 SRTP의 명세를 정의하기 위한 프로토콜로 쉽게 말해 SRTP방식에서 Key 관리 기능을 한다고 보면 된다. MIKEY는 암호화된 RTP, 즉 SRTP를 전송하여 그 자체가 무결성 및 인증을 제공한다.



[Fig. 11] MIKEY Call Flow

4.3 구체적 대응 방안

따라서 이 논문에서는 아래의 그림과 같이 인증을 위한 OTD와 암호화를 위한 MIKEY를 활용한 대응 방안을 제시한다. 기존의 일회용 패스워드 기반 인증 방법의 특성을 적용하여 모바일 단말에서의 부가 서비스 사용시 인증 과정에 적용할 수 있으며 이를 통해서 보안성을 향상시킬 수 있을 것으로 기대된다.



[Fig. 12] Proposed Mechanism using OTD and MIKEY

위에서 설명한 것과 같이 User A가 INVITE 패킷을 전송하게 되면 SSW는 User A가 맞는지 확인하기 위해 OTD를 전송한다. User A는 OTD를 확인하여 이를 적용한 새로운 INVITE 생성 및 그 안에 MIKEY를 넣어 User B와 안전하게 RTP를 주고받을 수 있게 한다. SSW는 User A가 보낸 INVITE 패킷 내용을 확인하여 OTD를 통해 User A를 확인한 후 User B에게 MIKEY가 들어있는 INVITE를 전송한다. 이를 통해 User A에 대한 인증 과정 및 User A와 User B가 서로 MIKEY를 서로 지니고 있게 된다. 이 때 지나가는 MIKEY는 OTD를 통해 암호화 되어 있으며 SSW는 OTD와 MIKEY를 둘 다 전송받게 된다. SSW는 OTD를 확인하는 것은 물론 복호화를 통해 얻은 MIKEY를 User B에게 전송하여 User A와 User B가 같은 MIKEY를 지닐 수 있도록 한다. 이후 연결 과정은 기본 과정과 동일하다.

이 같은 방식이 인증 및 무결성과 기밀성을 유지하는 만큼 Replay Attack이나 패킷 위변조, 도청 등의 취약점을 이용한 대부분의 공격을 사전에 차단할 수 있으며 사용자는 안전한 mVoIP 환경에서 통화를 할 수 있다.

5. 결론

본 연구에서는 현재 상용화되어 있는 대표적인 mVoIP 서비스에 대하여 조사 분석 및 대응 방안을 제시하였다. 스마트폰에서의 통화 및 mVoIP 기반으로 제공되는 통화 서비스 및 각 종 부가서비스를 대상으로 Call Flow를 통해 분석하였으며 이를 통해 mVoIP 서비스의 구조에 대해 알 수 있었다. 그 결과 대부분의 mVoIP 서비스가 암호화 및 인증 방식에 취약하며 대부분의 패킷에 있어서 내용이 그대로 드러나 데이터의 기밀성이 없이 송수신자의 정보 또한 쉽게 얻어낼 수 있다는 점을 알 수 있었다.

특히 대부분의 정보는 초기 연결 설정을 위해 지나는 INVITE 패킷을 통해 송수신자의 정보 외에 현재 연결요청에 대한 정보 및 각 연결 대상자의 상태까지 알 수 있었다. 또한 데이터 정보에 해당하는 RTP의 경우 정보를 얻는 것은 물론 위변조 또한 쉽게 할 수 있기 때문에 INVITE 패킷을 비롯하여 이를 이용한 재전송 공격이나 사칭 공격 등에 취약할 수 있다는 결과를 얻을 수 있었다.

그 결과 분석한 부가서비스를 토대로 서비스 과정의 전체구조와 공격 대상에게 피해를 줄 수 있는 주요 취약

점을 분석할 수 있었으며 이를 통해 취약성에 대한 대응 방안을 제시할 수 있었다.

REFERENCES

[1] Ji-Hun Kim, “VoIP Security Threats”, ASEC, 2008.
[2] JaeDeok Choi, etc, "Implementation of SIP based VoIP Security System", Journal of KICS, Vol. 3, No. 3, 2004.
[3] JaHyun Ku, "Vulnerability Analysis on VoIP Service", Journal of KIISC, Vol. 16, No. 1, pp. 60-63, 2006.
[4] JinBum Park, etc, “A Research on the Vulnerability and Response Mechanism against the VoIP Attack,”Journal of KIISC, Vol. 17, No. 5, 2007.
[5] YoungChan Shin, etc, "Performance Evaluation on VoIP Protocol", Journal of KIISC, Vol. 18, No. 3, 2008.
[6] Hemant Sengar. "VoIP Intrusion Detection Through Interacting Protocol State Machines", 2006.

Acknowledgement

본 논문은 학술대회 우수논문으로 선정된 것으로 본 논문의 일부 내용은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2012R1A1A2004573)

저자소개

조 식 완 (Sik-Whan Cho) [정회원]

- 2010년 2월 : 한신대학교 소프트웨어학과 졸업
- 2010년 2월 ~ 현재 : 한신대학교 일반대학원 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 모바일 보안

장 원 준 (Won-Jun Jang) [정회원]

- 2010년 2월 : 한신대학교 정보시스템공학과 졸업
- 2010년 2월 ~ 현재 : 한신대학교 일반대학원 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 스마트폰 보안

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 전산과학과 졸업
- 1996년 2월 : 고려대학교 일반대학원 전산과학과 석사
- 1999년 2월 : 고려대학교 일반대학원 전산과학과 박사
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 정교수

<관심분야> : 정보보호, 포렌식, 네트워크 보안, 바이오정보보호, 스마트단말 보안